Question 1

An administrator is configuring cisco ISE lo authenticate users logging into network devices using TACACS+ The administrator is not seeing any o the authentication in the TACACS+ live logs. Which action ensures the users are able to log into the network devices?

Options:

A- Enable the device administration service in the Administration persona

B- Enable the session services in the administration persona

C- Enable the service sessions in the PSN persona.

D- Enable the device administration service in the PSN persona.

Answer:

D

Explanation:

https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/m_ise_tacacs_device_admin.html

Question 2

Which RADIUS attribute is used to dynamically assign the inactivity active timer for MAB users from the Cisco ISE node'?

Options:

A- radius-server timeout

B- session-timeout

C- idle-timeout

D- termination-action

Answer:

C

Question 3

An administrator enables the profiling service for Cisco ISE to use for authorization policies while in closed mode. When the endpoints connect, they receive limited access so that the profiling probes can gather information and Cisco ISE can assign the correct profiles. They are using the default values within Cisco ISE. but the devices do not change their access due to the new profile. What is the problem'?

Options:

A- In closed mode, profiling does not work unless CDP is enabled.

B- The profiling probes are not able to collect enough information to change the device profile

C- The profiler feed is not downloading new information so the profiler is inactive

D- The default profiler configuration is set to No CoA for the reauthentication setting

Answer:

D

Question 4

Which Cisco ISE deployment model provides redundancy by having every node in the deployment configured with the Administration. Policy Service, and Monitoring personas to protect from a complete node failure?

Options:

A- distributed

B- dispersed

C- two-node

D- hybrid

Answer:

A

Question 5

Question Type: MultipleChoice

An administrator is configuring RADIUS on a Cisco switch with a key set to Cisc403012128 but is receiving the error "Authentication failed: 22040 Wrong password or invalid shared secret. "what must be done to address this issue?

Options:

A- Add the network device as a NAD inside Cisco ISE using the existing key.

B- Configure the key on the Cisco ISE instead of the Cisco switch.

C- Use a key that is between eight and ten characters.

D- Validate that the key is correct on both the Cisco switch as well as Cisco ISE.

Answer:

D

Question 6

Question Type: **MultipleChoice**

An adminstrator is migrating device administration access to Cisco ISE from the legacy TACACS+ solution that used only privilege 1 and 15 access levels. The organization requires more granular controls of the privileges and wants to customize access levels 2-5 to correspond with different roles and access needs. Besides defining a new shell profile in Cisco ISE. what must be done to accomplish this configuration?

Options:

A- Enable the privilege levels in Cisco ISE

B- Enable the privilege levels in the IOS devices.

C- Define the command privileges for levels 2-5 in the IOS devices

D- Define the command privileges for levels 2-5 in Cisco ISE

Answer:

B

Explanation:

https://learningnetwork.cisco.com/s/blogs/a0D3i000002eeWTEAY/cisco-ios-privilege-levels

Question 7

Question Type: **MultipleChoice**

An engineer is configuring a dedicated SSID for onboarding devices. Which SSID type accomplishes this configuration?

Options:

A- dual

B- hidden

C- broadcast

D- guest

Answer:

A

Explanation:

https://community.cisco.com/t5/security-documents/ise-byod-dual-vs-single-ssid-onboarding/ta-p/3641422

https://www.youtube.com/watch?v=HH_Xasqd9k4&ab_channel=CiscoISE-IdentityServicesEngine

http://www.labminutes.com/sec0053_ise_1_1_byod_wireless_onboarding_dual_ssid